REMARKS

Applicants respectfully request reconsideration of the rejection of this application as examined pursuant to the office action of June 12, 2006. In the office action, Claims 1-27 were examined. No claims have been cancelled and no new claims have been added. Claims 1-27 remain pending after entry of this Amendment.

Claims 1-27 were rejected under 35 USC § 102(b) as being unpatentable over a published PCT application to Huff et al., WIPO Publication No. WO99/57625 ("Huff").

The Applicants have taken this opportunity to amend the claims to distinguish the present invention more clearly from the system of the cited reference. Primarily, independent method Claim 1 has been amended to state that: 1) monitoring of the network system for intrusions is performed using one or more devices of the network infrastructure; 2) the source of the intrusion is made by identifying one or more signal transferring devices of the network infrastructure; and 3) response to the detected intrusion is performed by configuring the one or more signal transferring devices of the network infrastructure with policy changes. Similarly, independent system Claim 16 has been amended to state that the system includes intrusion detection by one or more network infrastructure devices and intrusion response is achieved through one or more signal transferring devices of the network infrastructure.

Applicants respectfully suggest that the amendments made to the independent claims further distinguish the present invention from the system described in the cited reference.

The 35 USC § 102(b) Rejection

Claims 1-27 as filed were rejected as being anticipated by Huff. Applicants respectfully suggest that Huff is inapplicable to the present invention as described in the amended claims because Huff describes the use of software-based agents to perform the detection and change/chase missions described therein. The agents are distributed to all network end nodes and particularly the computers (e.g., personal computer 112) where examination and changes take place. The end nodes that Huff clearly uses for agent insertion and operation are the equivalent of the attached functions described in the present application. That is, they are the functions seeking access to and usage of the services of the network infrastructure. They are not the network infrastructure devices.

Applicants respectfully disagree with the examiner's position stated in paragraph 18 of the June 12, 2006, office action that Huff foresees implementation of the agents in network devices that may be characterized as signal transferring devices, such as switches, for example. Huff states only that each node of the network must include the detection/change mission agents. In fact, Huff barely acknowledges the existence of the network infrastructure devices required to transfer signals through the network system, let alone that they should provide the detection and response functionality instead of all end nodes (attached functions). The closest indication to the inclusion of signal transferring devices in the Huff reference is the passing mention of the cable 102 as a connector.. It appears that the only type of signal transferring device even listed by Huff is an Internet Protocol router described as being part of the interface 118 in FIG. 1; not even part of the identified network to be protected. (See page 9, lines 12-15 of Huff.) The present invention focuses on use of the network infrastructure devices for detection and response. Huff simply does not.

The system described by Huff appears to make each and every end node of the network system an intrusion detector and responder. That arrangement requires that each and every end node of the network system accept an agent, much like the computer security systems generally commercially available. Further, as Huff indicates on page 15, lines 23-25 "It is important that the communication framework 410 and agent core framework 420 have full permission to use and access every resource on the host computer 108 or 112, to append, delete, modify or rewrite files." In other words, all attached functions must allow the agent full access for operational changes. It must be concluded, therefore, that any attached function not authorizing such transfer of control cannot gain access to the network system, or that an attached function could surreptitiously connect to the network with no mechanism in the network infrastructure to adapt to any sort of intrusion generated by such unauthorized "end node." Such a method of network protection would be difficult to establish and maintain.

The present invention, on the other hand, is directed to protection of the network system in a much more distinct and feasible manner. The present invention involves protection of the network infrastructure by devices of the network infrastructure rather than by agents inserted into end nodes attached to the network infrastructure. The method and related system of the present invention as described in the amended claims provide for detection of intrusions by one or more devices of the network infrastructure and response to such intrusions through policy changes

made at the signal transferring (or signal relay) devices of the network infrastructure. This arrangement enables the ability to target through which infrastructure device intrusion response occurs with minimal impact on the rest of the network, to focus on those attached functions affecting or affected by the intrusion, and maintains control of the response to the intrusion in the network infrastructure, rather than in reliance upon the security performance of individual attached functions. This is all achieved without requiring control over attached functions or the requirement to install an agent, which likely must be regularly updated to ensure reasonable network security, into each attached function.

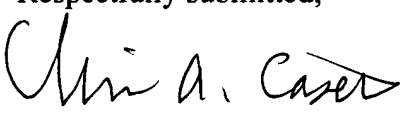
The present invention as described by the amended independent claims, teaches a system for intrusion response tailored to detecting through the network infrastructure, not agents of end nodes (attached functions) and responding through signal transferring devices of the network infrastructure, again, not through end nodes. The remaining dependent claims have been amended to conform with the amendments made to independent Claims 1 and 16. In view of the amendments made to the independent claims and the arguments presented herein, Applicants respectfully suggest that the 35 U.S.C. § 102(b) rejection of pending Claims 1-27 based on Huff has been successfully traversed. Withdrawal of that rejection is therefore requested.

CONCLUSION

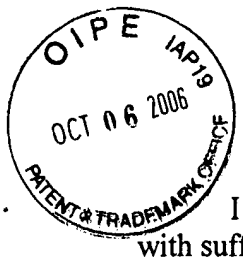
In view of the foregoing amendments made to the independent claims and the remarks made herein, Applicants respectfully suggest that the rejection under 35 § 102(b) has been successfully traversed. Allowance of pending Claims 1-27 is therefore requested.

By this amendment, no new claims have been added. Therefore, no additional filing fee is required.

Respectfully submitted,



Chris A. Caseiro, Reg. No. 34,304
Attorney for Applicants
Verrill & Dana, LLP
One Portland Square
Portland, ME 04112-0586
Tel. No. 207-253-4530



Certificate of Mailing

I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450, on October 2, 2006. It is hereby requested that this filing be granted a filing date of October 2, 2006.

Chris A. Caseiro